Atty. Dkt. No. 043034-0181

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Masao SHIMADA

Title: NETWORK INFORMATION DETECTION APPARATUS AND METHOD

Appl. No.: 10/802,738

Filing Date: 03/18/2004

Examiner: Unknown

Art Unit: Unknown

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

Japanese Patent Application No. 2003-074846
filed 03/19/2003.

Respectfully submitted,

Date: April 30, 2004

By _____ Reg. No. 43,438
David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年 ３月１９日

出 願 番 号
Application Number: 特願２００３－０７４８４６

[ST. 10/C]: [ＪＰ２００３－０７４８４６]

出 願 人
Applicant(s): 日本電気株式会社

２００４年 １月１３日

特許庁長官
Commissioner,
Japan Patent Office 今 井 康 夫

出証番号 出証特２００３－３１１０６０３

【書類名】　特許願
【整理番号】　34403245
【提出日】　平成15年 3月19日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/28
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　嶋田　昌生
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100097157
　【弁理士】
　【氏名又は名称】　桂木　雄二
【手数料の表示】
　【予納台帳番号】　024431
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9303562
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワーク情報検出装置および方法

【特許請求の範囲】

【請求項１】　ネットワークに接続されたデバイスのＩＰ(Internet Protocol)アドレスを検出するネットワーク情報検出装置において、

前記ネットワーク上の可能なＩＰアドレスから予め定められた個数ごとに選択されたＩＰアドレスから検査対象ＩＰアドレスを検出する検査対象検出手段と、

前記検出された検査対象ＩＰアドレスから目的とする対象デバイスのＩＰアドレスを検出するＩＰアドレス検出手段と、

前記ネットワーク上の可能なＩＰアドレスのすべてについて選択された場合および前記目的とする対象デバイスのＩＰアドレスが検出された場合のいずれかの場合にネットワーク情報検出動作を終了する制御手段と、

を有することを特徴とするネットワーク情報検出装置。

【請求項２】　前記ＩＰアドレス検出手段は、ＤＮＳ(Domain Name System)サーバのＩＰアドレスを検出するＤＮＳサーバ検出手段およびルータのＩＰアドレスを検出するルータ検出手段のうち少なくとも一方を含むことを特徴とする請求項１記載のネットワーク情報検出装置。

【請求項３】　前記ＩＰアドレス検出手段は、さらに、ＤＮＳサーバおよびルータ以外のサービスを提供するデバイスのＩＰアドレスを検出するサービス検出手段を含むことを特徴とする請求項２記載のネットワーク情報検出装置。

【請求項４】　少なくともＤＮＳ(Domain Name System)サーバを含むネットワーク上のＩＰ(Internet Protocol)アドレスを検出するネットワーク情報検出装置において、

前記ネットワーク上の可能なＩＰアドレスから１以上の検査対象ＩＰアドレスを検出する検査対象検出手段と、

前記１以上の検査対象ＩＰアドレスに対してＤＮＳクエリメッセージを送信し、そのレスポンスメッセージを受信するＤＮＳメッセージ送受信手段と、

前記レスポンスメッセージからＤＮＳレスポンスメッセージを識別し、ＤＮＳレスポンスメッセージから発信元のＤＮＳサーバのＩＰアドレスを検出するＤＮ

Ｓサーバ検出手段と、

を有することを特徴とするネットワーク情報検出装置。

【請求項５】　前記検査対象検出手段は、前記ネットワーク内の可能なＩＰアドレスから予め定められた個数ごとに選択されたＩＰアドレスに対してＡＲＰ(Address Resolution Protocol)要求を一括送信し、それに対するＡＲＰ応答から前記検査対象ＩＰアドレスを検出することを特徴とする請求項４記載のネットワーク情報検出装置。

【請求項６】　前記ＤＮＳクエリメッセージは、ＤＮＳプロトコルヘッダのＱＲビットをリセットした、スタンダードクエリ、インバースクエリ、サーバステータスリクエスト、および、アップデートの少なくとも１種類のメッセージであることを特徴とする請求項４記載のネットワーク情報検出装置。

【請求項７】　前記１以上の検査対象ＩＰアドレスに対してＩＣＭＰエコー要求メッセージを送信し、そのＩＣＭＰレスポンスメッセージを受信するＩＣＭＰメッセージ送受信手段と、

前記ＩＣＭＰレスポンスメッセージから発信元のルータのＩＰアドレスを検出するルータ検出手段と、

をさらに有することを特徴とする請求項４または５に記載のネットワーク情報検出装置。

【請求項８】　前記ＩＣＭＰレスポンスメッセージはＩＣＭＰ経路変更要求メッセージおよびＩＣＭＰ時間切れメッセージのいずれかであることを特徴とする請求項７記載のネットワーク情報検出装置。

【請求項９】　ネットワークに接続されたデバイスのＩＰ(Internet Protocol)アドレスを検出するネットワーク情報検出方法において、

前記ネットワーク上の可能なＩＰアドレスから予め定められた個数ごとに選択し、

前記選択された予め定められた個数のＩＰアドレスから検査対象ＩＰアドレスを検出し、

前記検出された検査対象ＩＰアドレスから目的とする対象デバイスのＩＰアドレスを検出し、

前記ネットワーク上の可能なＩＰアドレスのすべてについて選択された場合および前記目的とする対象デバイスのＩＰアドレスが検出された場合のいずれかの場合にネットワーク情報検出動作を終了する、

ことを特徴とするネットワーク情報検出方法。

【請求項１０】　少なくともＤＮＳ(Domain Name System)サーバを含むネットワーク上のＩＰ(Internet Protocol)アドレスを検出するネットワーク情報検出方法において、

前記ネットワーク上の可能なＩＰアドレスから１以上の検査対象ＩＰアドレスを検出し、

前記１以上の検査対象ＩＰアドレスに対して送信されたＤＮＳクエリメッセージに対するレスポンスメッセージを受信し、

前記レスポンスメッセージからＤＮＳレスポンスメッセージを識別して当該ＤＮＳレスポンスメッセージから発信元のＤＮＳサーバのＩＰアドレスを検出する、

を有することを特徴とするネットワーク情報検出方法。

【請求項１１】　前記検査対象ＩＰアドレス検出ステップは、

前記ネットワーク内の可能なＩＰアドレスから予め定められた個数ごとに選択されたＩＰアドレスに対してＡＲＰ(Address Resolution Protocol)要求を一括送信し、

前記ＡＲＰ要求に対するＡＲＰ応答から前記検査対象ＩＰアドレスを検出する、

ことを特徴とする請求項１０記載のネットワーク情報検出方法。

【請求項１２】　コンピュータに、ネットワークに接続されたデバイスのＩＰ(Internet Protocol)アドレスを検出するネットワーク情報検出動作を指令するプログラムにおいて、

前記ネットワーク上の可能なＩＰアドレスから予め定められた個数ごとに選択するステップと、

前記選択された予め定められた個数のＩＰアドレスから検査対象ＩＰアドレスを検出するステップと、

前記検出された検査対象ＩＰアドレスから目的とする対象デバイスのＩＰアドレスを検出するステップと、

前記ネットワーク上の可能なＩＰアドレスのすべてについて選択された場合および前記目的とする対象デバイスのＩＰアドレスが検出された場合のいずれかの場合にネットワーク情報検出動作を終了するステップと、

を有することを特徴とするネットワーク情報検出プログラム。

【請求項１３】　コンピュータに、少なくともＤＮＳ(Domain Name System)サーバを含むネットワーク上のＩＰ(Internet Protocol)アドレスを検出するネットワーク情報検出動作を指令するプログラムにおいて、

前記ネットワーク上の可能なＩＰアドレスから１以上の検査対象ＩＰアドレスを検出するステップと、

前記１以上の検査対象ＩＰアドレスに対して送信されたＤＮＳクエリメッセージに対するレスポンスメッセージを受信するステップと、

前記レスポンスメッセージからＤＮＳレスポンスメッセージを識別して当該ＤＮＳレスポンスメッセージから発信元のＤＮＳサーバのＩＰアドレスを検出するステップと、

を有することを特徴とするネットワーク情報検出プログラム。

【請求項１４】　前記検査対象ＩＰアドレス検出ステップは、

前記ネットワーク内の可能なＩＰアドレスから予め定められた個数ごとに選択されたＩＰアドレスに対してＡＲＰ(Address Resolution Protocol)要求を一括送信するステップと、

前記ＡＲＰ要求に対するＡＲＰ応答から前記検査対象ＩＰアドレスを検出するステップと、

を有することを特徴とする請求項１３記載のネットワーク情報検出プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はネットワークシステムに係り、特に、ネットワーク情報を自動取得す

るネットワーク情報検出装置および方法に関する。

【０００２】

【従来の技術】

コンピュータをネットワークに接続するには、ルータのＩＰ(Internet Protocol)アドレスやＤＮＳ(Domain Name System)のＩＰアドレス等のネットワーク情報をコンピュータに設定する必要がある。このようなネットワーク情報は手動で設定することもできるが、人手による設定にはネットワークの知識を必要とし、ネットワーク情報を調査する手間もかかる。また、誤ってネットワーク情報を設定した場合はネットワーク全体を混乱させることもありうる。

【０００３】

他方、ＤＨＣＰ(Dynamic Host Configuration Protocol)サーバが存在する場合には、ネットワーク情報をＤＨＣＰサーバから取得することができるが、このようなネットワーク情報の自動取得を行うには、ネットワーク情報の提供を目的としたサーバを構築しなければならない。

【０００４】

特開２００２－１９０８１１号公報には、ネットワーク上の装置のＩＰアドレスを自動的に取得する方法の一例が開示されている。この従来の方法では、ネットワーク情報をＤＨＣＰサーバから取得できない場合に、ネットワーク・トラフィックを分析して有効なサブネットを決定し（段落番号００１８～００２１）、そのなかでＩＣＭＰ(Internet Control Message Protocol)ルータセレクションメッセージを用いてデフォルトルータを、ＳＮＭＰ(Simple Network Management Protocol)のＤＮＳ発見要求を用いてＤＮＳサーバをそれぞれ検出している（段落番号００２５～００２７）。

【０００５】

【特許文献１】

特開２００２－１９０８１１号公報（段落番号００２５～００２７、要約、図３～５）。

【０００６】

【発明が解決しようとする課題】

しかしながら、特許文献１に開示されたＩＰ構成自動取得方法では、ＲＦＣ１２５６に記述されているルータのＩＰアドレス検出方法をそのまま用いているだけであり、ルータ検出の高速化については考慮されていない。また、ＩＣＭＰルータセレクションをサポートしていないルータが存在するために、従来の方法ではルータを検出できない場合がある。

【０００７】

同様に、上記従来の方法では、ＤＮＳサーバ検出の高速化についても考慮されていない。また、ＳＮＭＰのＤＮＳ発見要求をサポートしていないＤＮＳサーバがあるために、ＤＮＳサーバを検出できない場合がある。

【０００８】

本発明の目的は、ネットワーク情報を提供するサーバ機能を必要とせずに、ネットワーク情報を自動かつ高速で取得することができるネットワーク情報検出装置及び方法を提供することにある。

【０００９】

本発明の他の目的は、ネットワーク情報を確実に取得することができるネットワーク情報検出装置及び方法を提供することにある。

【００１０】

【課題を解決するための手段】

本発明の第１の側面によるネットワーク情報検出装置は、ネットワークに接続されたデバイスのＩＰ(Internet Protocol)アドレスを検出するネットワーク情報検出装置であって、前記ネットワーク上の可能なＩＰアドレスから予め定められた個数ごとに選択されたＩＰアドレスから検査対象ＩＰアドレスを検出する検査対象検出手段と、前記検出された検査対象ＩＰアドレスから目的とする対象デバイスのＩＰアドレスを検出するＩＰアドレス検出手段と、前記ネットワーク上の可能なＩＰアドレスのすべてについて選択された場合および前記目的とする対象デバイスのＩＰアドレスが検出された場合のいずれかの場合にネットワーク情報検出動作を終了する制御手段と、を有することを特徴とする。

【００１１】

本発明の第２の側面によるネットワーク情報検出装置は、少なくともＤＮＳ(D

omain Name System)サーバを含むネットワーク上のＩＰ(Internet Protocol)アドレスを検出するネットワーク情報検出装置であって、前記ネットワーク上の可能なＩＰアドレスから１以上の検査対象ＩＰアドレスを検出する検査対象検出手段と、前記１以上の検査対象ＩＰアドレスに対してＤＮＳクエリメッセージを送信し、そのレスポンスメッセージを受信するＤＮＳメッセージ送受信手段と、前記レスポンスメッセージからＤＮＳレスポンスメッセージを識別し、ＤＮＳレスポンスメッセージから発信元のＤＮＳサーバのＩＰアドレスを検出するＤＮＳサーバ検出手段と、を有することを特徴とする。

【００１２】

前記検査対象検出手段は、前記ネットワーク内の可能なＩＰアドレスから予め定められた個数ごとに選択されたＩＰアドレスに対してＡＲＰ(Address Resolution Protocol)要求を一括送信し、それに対するＡＲＰ応答から前記検査対象ＩＰアドレスを検出することを特徴とする。

【００１３】

前記ＤＮＳクエリメッセージは、ＤＮＳプロトコルヘッダのＱＲビットをリセットした、スタンダードクエリ、インバースクエリ、サーバステータスリクエスト、および、アップデートの少なくとも１種類のメッセージであることを特徴とする。

【００１４】

さらに、前記ネットワーク情報検出装置は、前記１以上の検査対象ＩＰアドレスに対してＩＣＭＰエコー要求メッセージを送信しそのＩＣＭＰレスポンスメッセージを受信するＩＣＭＰメッセージ送受信手段と、前記ＩＣＭＰレスポンスメッセージから発信元のルータのＩＰアドレスを検出するルータ検出手段と、を有することを特徴とする。前記ＩＣＭＰレスポンスメッセージはＩＣＭＰ経路変更要求メッセージおよびＩＣＭＰ時間切れメッセージのいずれかであることを特徴とする。

【００１５】

【発明の実施の形態】

図１は本発明によるネットワーク情報検出装置を含むネットワークの一例を示

す概略的構成図である。この例では、ネットワーク伝送路１０に、ネットワーク情報検出装置２０、ホストＡ３０、 ホストＢ４０、ＤＮＳサーバ５０およびルータ６０などの複数のネットワークデバイスが接続されている。本発明によるネットワーク情報検出装置２０は、このサブネットからＤＮＳサーバ５０および／またはルータ６０を検出する。

【００１６】

図２は本発明の第１実施形態によるネットワーク情報検出装置を示すブロック構成図である。本実施形態によるネットワーク情報検出装置２０は、ネットワーク伝送路１０に接続するためのネットワークインタフェース部２１を有し、ネットワークインタフェース部２１はＡＲＰ要求送信部２３、ＡＲＰ応答受信部２４、ルータ検出部２５、ＤＮＳサーバ検出部２６、および、ネットワーク情報送信部２８に接続され、後述するようにＩＰパケットまたはＡＲＰパケットの送受信を行う。ＡＲＰ応答受信部２４は、後述するように、ルータ検出部２５およびＤＮＳサーバ検出部２６に接続され、ルータ検出部２５、ＤＮＳサーバ検出部２６およびネットワーク情報送信部２８はネットワーク情報設定部２７にそれぞれ接続されている。また、ネットワーク情報検出装置２０の全体的動作は制御部２２により制御される。

【００１７】

ＡＲＰ要求送信部２３は、制御部２２の制御の下で、サブネット内の予め定めた個数のＩＰアドレスに対して一括してＡＲＰ要求パケットを送信する処理を繰り返す（詳しくは後述する）。なお、ＩＰアドレスの構成は図７に、ＡＲＰ要求パケットのフォーマットは図１１にそれぞれ示す。

【００１８】

ＡＲＰ応答受信部２４は、ＡＲＰ要求送信部２３が送信したＡＲＰ要求パケットに対するＡＲＰ応答パケットをホストＡ３０、ホストＢ４０、ＤＮＳサーバ５０、または、ルータ６０から受信する。当該ＡＲＰ応答パケットの送信元ＩＰアドレスはルータ検出部２５およびＤＮＳサーバ検出部２６へ出力される。ＡＲＰ応答パケットのフォーマットは図１１に示す。

【００１９】

ルータ検出部２５は、ＡＲＰ応答受信部２４から入力した送信元ＩＰアドレスをルータ検出の対象ＩＰアドレスとし、予め定めた個数のルータ検出対象ＩＰアドレスごとにルータ特徴確認を繰り返すことによりルータ６０を検出する（詳しくは後述する）。検出されたルータ６０のＩＰアドレスはネットワーク情報設定部２７に出力される。

【００２０】

ＤＮＳサーバ検出部２６は、ＡＲＰ応答受信部２４から入力した送信元ＩＰアドレスをＤＮＳサーバ検出の対象ＩＰアドレスとし、予め定めた個数のＤＮＳサーバ検出対象ＩＰアドレスごとにＤＮＳサーバ特徴確認を繰り返すことによりＤＮＳサーバ５０を検出する（詳しくは後述する）。検出されたＤＮＳサーバのＩＰアドレスはネットワーク情報設定部２７に出力される。

【００２１】

ネットワーク情報設定部２７は、ルータ検出部２５が検出したルータＩＰアドレスおよびＤＮＳサーバ検出部２６が検出したＤＮＳサーバＩＰアドレスの少なくとも一方を、自己の装置に設定したり、または、他のネットワーク装置で利用可能とするためにネットワーク情報送信部２８へ出力する。

【００２２】

ネットワーク情報送信部２８は、ネットワーク情報設定部２７から入力したルータＩＰアドレスおよび／またはＤＮＳサーバＩＰアドレスを他のネットワーク装置で利用可能とするためにネットワークインターフェース部２１を通して送信する。

【００２３】

ネットワーク伝送路１０上を流れるパケットは、たとえばＬＡＮがEthernet（登録商標、IEEE802.３）であれば図８に示すフォーマットのデータリンク層のパケットとなり、ＩＰパケットであれば図９に示すフォーマットとなり、ＡＲＰパケットであれば図１１に示すフォーマットとなる。

【００２４】

上記ネットワーク情報検出装置２０には、ルータ検出部２５およびＤＮＳサーバ検出部２６が両方も受けられているが、一方だけでもよい。

【００２５】

なお、図２には図示されていないが、本実施形態によるネットワーク情報検出装置２０は、ネットワーク上で上記以外のサービスまたは機能を実行している装置のＩＰアドレスを検出するサービス検出部を設けることもできる。

【００２６】

ネットワーク情報検出動作

以下、本実施形態の動作を図３～図５に示すフローチャートおよび図８～図１２に示すパケットフォーマットを参照しながら詳細に説明する。

【００２７】

図３は本発明による第１実施形態のルータ／ＤＮＳサーバ検出動作を全体的に示すフローチャートである。まず制御部２２は、予め保存しているサブネット情報に基づいて、ＡＲＰ要求送信部２３がサブネットの全てのＩＰアドレスに対してＡＲＰ要求パケット（図１１参照）を発行したか否かを判定し（ステップＳ２００１）、真（Ｙｅｓ）の場合は終了する。

【００２８】

サブネットの全てのＩＰアドレスに対してＡＲＰ要求パケットを発行していない場合には（ステップＳ２００１のＮｏ）、サブネット内の予め定めた個数のＩＰアドレスごとにＡＲＰ要求パケットを一括送信する（ステップＳ２００２）。具体的には、サブネットマスクが２５５．２５５．２５５．０、ネットワークアドレスが１９２．１６８．１．０とし、一括送信するＩＰアドレス数を１００個と仮定すれば、第一回目のステップＳ２００２の実行時には１９２．１６８．１．１～１９２．１６８．１．１００のＩＰアドレスに対してＡＲＰ要求パケットを送信し、第二回目の実行時には１９２．１６８．１．１０１～１９２．１６８．１．２００のＩＰアドレスに対して、第三回目の実行時には１９２．１６８．１．２０１～１９２．１６８．１．２５４のＩＰアドレスに対して、それぞれＡＲＰ要求を送信する。

【００２９】

制御部２２は、ＡＲＰ要求の応答として１つ以上のＡＲＰ応答パケット（図１１参照）を受信したかどうかを判定し（ステップＳ２００３）、なんらＡＲＰ応

答がない場合は（ステップＳ２００３のＮｏ）、ステップＳ２００１に戻る。

【００３０】

１つ以上のＡＲＰ応答パケットを受信した場合は（ステップＳ２００３のＹｅｓ）、ルータ検出が終了したかどうかを判定する（ステップＳ２００４）。ルータ検出が終了していなければ（ステップＳ２００４のＮｏ）ルータの特徴確認（ステップＳ２００５）を実行し、終了していれば（ステップＳ２００４のＹｅｓ）ルータ特徴確認をスキップして、ＤＮＳサーバ検出が終了したかどうかを判定する（ステップＳ２００６）。

【００３１】

ＤＮＳサーバ検出が終了していなければ（ステップＳ２００６のＮｏ）ＤＮＳサーバの特徴確認（ステップＳ２００７）を実行して、終了していれば（ステップＳ２００６のＹｅｓ）、ＤＮＳサーバの特徴確認をスキップして、ルータおよびＤＮＳサーバを検出したかどうかを判定する（ステップＳ２００８）。

【００３２】

ルータおよびＤＮＳサーバを検出した場合には（ステップＳ２００８のＹｅｓ）、処理を終了する。ルータおよびＤＮＳサーバを検出していない場合には（ステップＳ２００８のＮｏ）、ステップＳ２００１に戻り、以上の動作をサブネットの全てのＩＰアドレスに対してＡＲＰ要求パケットを発行するまで、あるいは、ルータおよびＤＮＳサーバを検出するまで、繰り返す。

【００３３】

なお、サービス検出部を有する場合には、サブネット内の予め定めた個数のＩＰアドレスに対してＡＲＰ要求パケットを一括発行し、その応答であるＡＲＰ応答パケットに含まれる送信元ＩＰアドレスに対して、サービス検出あるいは機能検出を行ってもよい。

【００３４】

（１）ルータ特徴確認

図４は本発明の第１実施形態におけるルータ検出部のルータ特徴確認動作の一例を示すフローチャートである。まず、ルータの検査対象ＩＰアドレスは、ＡＲＰ応答受信部２４が受信した全てのＡＲＰ応答パケットにそれぞれ含まれる送信

元ＩＰアドレスである。これらルータ検査対象ＩＰアドレスを入力すると（ステップＳ２０２０）、全てのルータ検査対象ＩＰアドレスに対してルータ特徴確認を行なったかどうかを判定し（ステップＳ２０２１）、すべて終了していれば（ステップＳ２０２１のＹｅｓ）、ルータ特徴確認動作を終了する。

【００３５】

検査すべきルータ検査対象ＩＰアドレスが残っていれば（ステップＳ２０２１のＮｏ）、ＴＴＬ(Time To Live)が所望の値に設定されたＩＣＭＰエコー要求パケット（図１０（Ａ）参照）を予め定めた個数のルータ検査対象ＩＰアドレスへ一括送信する（ステップＳ２０２２）。ここでは、ＴＴＬ＝２、すなわち通過可能ルータ段数が２であるとする。

【００３６】

例えば、ルータ検査対象ＩＰアドレスが１９２．１６８．１．１０～１９２．１６８．１．２４、および、１９２．１６８．１．４０～１９２．１６８．１．５１で、１０個のＩＰアドレスに一括してルータの特徴確認を行なう場合には、ステップＳ２０２２の実行は、第一回目に１９２．１６８．１．１０～１９２．１６８．１．１９に対して一括してＩＣＭＰエコー要求を送信し、第二回目に１９２．１６８．１．２０～１９２．１６８．１．２４と１９２．１６８．１．４０～１９２．１６８．１．４４とに対して一括してＩＣＭＰエコー要求を送信し、第三回目に１９２．１６８．１．４５～１９２．１６８．１．５１に対して一括してＩＣＭＰエコー要求を送信する。

【００３７】

ＩＣＭＰエコー要求パケットを一括送信すると、規定時間内に当該ＩＣＭＰエコー要求に対するＩＣＭＰ経路変更要求メッセージ（図１０（Ｃ）参照）を受信したかどうかを判定する（ステップＳ２０２３）。

【００３８】

ＩＣＭＰ経路変更要求メッセージを受信しなかった場合は（ステップＳ２０２３のＮｏ）、規定時間内に当該ＩＣＭＰエコー要求に対するＩＣＭＰ時間切れメッセージ（図１０（Ｂ））を受信したかどうかを判定する（ステップＳ２０２４）。受信しなかった場合は（ステップＳ２０２４のＮｏ）、ステップＳ２０２１

に戻る。　規定時間内にＩＣＭＰ時間切れメッセージを受信した場合は（ステップＳ２０２４のＹｅｓ）、当該時間切れメッセージパケットが含む送信元ＩＰアドレスをルータのＩＰアドレスであると判断して（ステップＳ２０２５）、ルータ特徴確認動作を終了する。

【００３９】

ＩＣＭＰ経路変更要求メッセージを受信した場合は（ステップＳ２０２３のＹｅｓ）、当該経路変更要求メッセージが含むルータＩＰアドレスをルータのＩＰアドレスであると判断して（ステップＳ２０２６）、ルータ特徴確認動作を終了する。

【００４０】

このように、所定のＴＴＬ設定されたＩＣＭＰエコー要求パケットを送信し、規定時間内に受信したＩＣＭＰ経路変更要求やＩＣＭＰ時間切れメッセージによってルータ検出を行うために、ルータの高速検出が可能となる。また、ルータはＩＣＭＰ時間切れメッセージ機能を必ずサポートしているために、確実なルータ検出が可能となる。

【００４１】

（２）ＤＮＳサーバ特徴確認

図５は本発明の第１実施形態におけるＤＮＳサーバ検出部のＤＮＳサーバ特徴確認動作の一例を示すフローチャートである。まず、ＤＮＳサーバの検査対象ＩＰアドレスは、ＡＲＰ応答受信部２４が受信した全てのＡＲＰ応答パケットにそれぞれ含まれる送信元ＩＰアドレスである。これらＤＮＳサーバ検査対象ＩＰアドレスを入力すると（ステップＳ２０４０）、全てのＤＮＳサーバの検査対象ＩＰアドレスに対してＤＮＳサーバ特徴確認を行なったかどうかを判定し（ステップＳ２０４１）、すべて終了していれば（ステップＳ２０４１のＹｅｓ）、ＤＮＳサーバ特徴確認動作を終了する。

【００４２】

検査すべきＤＮＳサーバ検査対象ＩＰアドレスが残っている場合は（ステップＳ２０４１のＮｏ）、ＱＲ（質問／回答）ビットをリセットしたＤＮＳクエリ（図１２参照）を予め定めた個数のＤＮＳサーバ検査対象ＩＰアドレスに対して一

括送信する（ステップＳ２０４２）。このＱＲビットをリセットしたＤＮＳクエリは、スタンダードクエリ（ＯＰＣＯＤＥ＝０）、インバースクエリ（ＯＰＣＯＤＥ＝１）、サーバステータスリクエスト（ＯＰＣＯＤＥ＝２）、あるいは、アップデート等のクエリメッセージである。

【００４３】

一括送信に関しては、例えばＤＮＳサーバ検査対象ＩＰアドレスが１９２．１６８．１．１０～１９２．１６８．１．２４、および、１９２．１６８．１．４０～１９２．１６８．１．５１で、１０個のＩＰアドレスに一括してＤＮＳサーバの特徴確認を行なう場合には、、第一回目に１９２．１６８．１．１０～１９２．１６８．１．１９に対して一括して前記ＤＮＳクエリを送信し、第二回目に１９２．１６８．１．２０～１９２．１６８．１．２４と、１９２．１６８．１．４０～１９２．１６８．１．４４とに対して一括して前記ＤＮＳクエリを送信し、第三回目に１９２．１６８．１．４５～１９２．１６８．１．５１に対して一括して前記ＤＮＳクエリを送信する。

【００４４】

ＤＮＳクエリを一括送信すると、規定時間内に当該ＤＮＳクエリに対するＤＮＳレスポンスを受信したかどうかを判定する（ステップＳ２０４３）。受信しなかった場合は（ステップＳ２０４３のＮｏ）、ステップＳ２０４１に戻る。規定時間内に当該ＤＮＳクエリに対するＤＮＳレスポンスを受信した場合は（ステップＳ２０４３のＹｅｓ）、ＤＮＳサーバのＩＰアドレスは当該ＤＮＳレスポンスパケットが含む送信元ＩＰアドレスであると判断し（ステップＳ２０４５）、ＤＮＳサーバ確認動作を終了する。

【００４５】

このように、ＤＮＳプロトコルのクエリメッセージを送信し、規定時間内に受信したそのレスポンスによってＤＮＳサーバを検出するために、ＤＮＳサーバの高速検出が可能となる。また、ＤＮＳサーバは、受信したクエリメッセージに対するレスポンス機能を必ずサポートしているために、確実なＤＮＳサーバ検出が可能となる。

【００４６】

図６は本発明の第２実施形態によるネットワーク情報検出装置を示すブロック構成図である。本実施形態によるネットワーク情報検出装置２０は、ネットワーク伝送路１０に接続するためのネットワークインタフェース２０１と、上述したＩＰパケットあるいはＡＲＰパケットを送受信するための送受信制御部２０２とを有し、プログラム制御プロセッサ２０３が上述したネットワーク情報の検出および設定を制御する。

【００４７】

プログラム制御プロセッサ２０３は、プログラムメモリ２０４に格納されたルータ検出プログラム、ＤＮＳサーバ検出プログラム、および、必要なサービス検出プログラムをそれぞれ読み出して実行することにより、上記図３～図５に示すネットワーク情報検出動作を行うことができる。こうして検出されたネットワーク情報はネットワーク情報メモリ２０５に格納され、自装置へ設定される。あるいは、ネットワーク上の他の装置の設定のために送信される。プログラム制御プロセッサ２０３により実行されるネットワーク情報検出動作は、図３～図５によりすでに説明した通りであるから、ここでは省略する。

【００４８】

【発明の効果】

以上詳細に説明したように、本発明によれば、ネットワーク上の可能なＩＰアドレスから予め定められた個数のＩＰアドレスを順次選択し、選択された予め定められた個数のＩＰアドレスから検査対象ＩＰアドレスを検出し、前記検出された検査対象ＩＰアドレスから目的とする対象デバイスのＩＰアドレスを検出することで、ＩＰアドレスの高速検出が可能となる。

【００４９】

また、本発明によれば、ＩＣＭＰエコー要求の応答であるＩＣＭＰ経路変更要求やＩＣＭＰ時間切れメッセージによってルータ検出を行うために、ルータの高速検出が可能となる。また、ルータはＩＣＭＰ時間切れメッセージ機能を必ずサポートしているために、確実なルータ検出が可能となる。

【００５０】

さらに、本発明によれば、ＤＮＳプロトコルのクエリメッセージに対するレス

ポンスによってＤＮＳサーバを検出するために、ＤＮＳサーバの高速検出が可能となる。また、ＤＮＳサーバは、受信したクエリメッセージに対するレスポンス機能を必ずサポートしているために、確実なＤＮＳサーバ検出が可能となる。

【００５１】

このように、ＤＮＳサーバのＩＰアドレスの検出およびルータのＩＰアドレスの検出を高速に自動で行うため、ユーザの待ち時間が少なく、また、ユーザの手作業でのＤＮＳサーバ／ルータＩＰアドレスの入力作業が不要となり、また間違えて入力した場合のネットワークの混乱や負荷の増大を防ぐことができる。とくに、本発明によるネットワーク情報検出装置は、販売店で購入してきたネットワーク装置をユーザのネットワークに接続したり、ネットワーク装置がネットワークを移動する場合に有効である。

【図面の簡単な説明】

【図１】

本発明によるネットワーク情報検出装置を含むネットワークの一例を示す概略的構成図である。

【図２】

本発明の第１実施形態によるネットワーク情報検出装置を示すブロック構成図である。

【図３】

本発明による第１実施形態のルータ／ＤＮＳサーバ検出動作を全体的に示すフローチャートである。

【図４】

本発明の第１実施形態におけるルータ検出部のルータ特徴確認動作の一例を示すフローチャートである。

【図５】

本発明の第１実施形態におけるＤＮＳサーバ検出部のＤＮＳサーバ特徴確認動作の一例を示すフローチャートである。

【図６】

本発明の第２実施形態によるネットワーク情報検出装置を示すブロック構成図

である。

【図７】

ＩＰアドレスのフォーマットを示す図である。

【図８】

イーサネットパケットのフォーマットを示す図である。

【図９】

ＩＰパケットのフォーマットを示す図である。

【図１０】

（Ａ）はＩＣＭＰエコー要求／応答パケットのフォーマットを示す図、（Ｂ）はＩＣＭＰ時間切れ通知パケットのフォーマットを示す図、（Ｃ）はＩＣＭＰ経路変更要求パケットのフォーマットを示す図である。

【図１１】

ＡＲＰパケットのフォーマットを示す図である。

【図１２】

ＤＮＳプロトコルヘッダのフォーマットを示す図である。

【符号の説明】

１０　ネットワーク伝送路

２０　ネットワーク情報検出装置

３０　ホストＡ

４０　ホストＢ

５０　ＤＮＳサーバ

６０　ルータ

２１　ネットワークインタフェース部

２３　ＡＲＰ要求送信部

２４　ＡＲＰ応答受信部

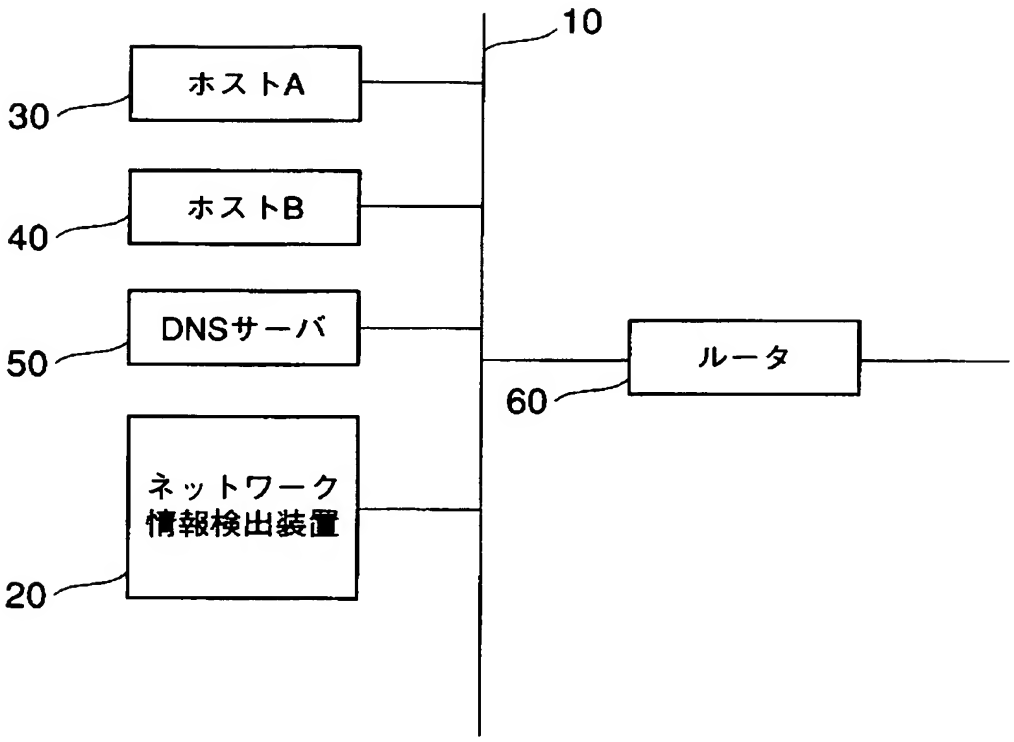
２５　ルータ検出部

２６　ＤＮＳサーバ検出部

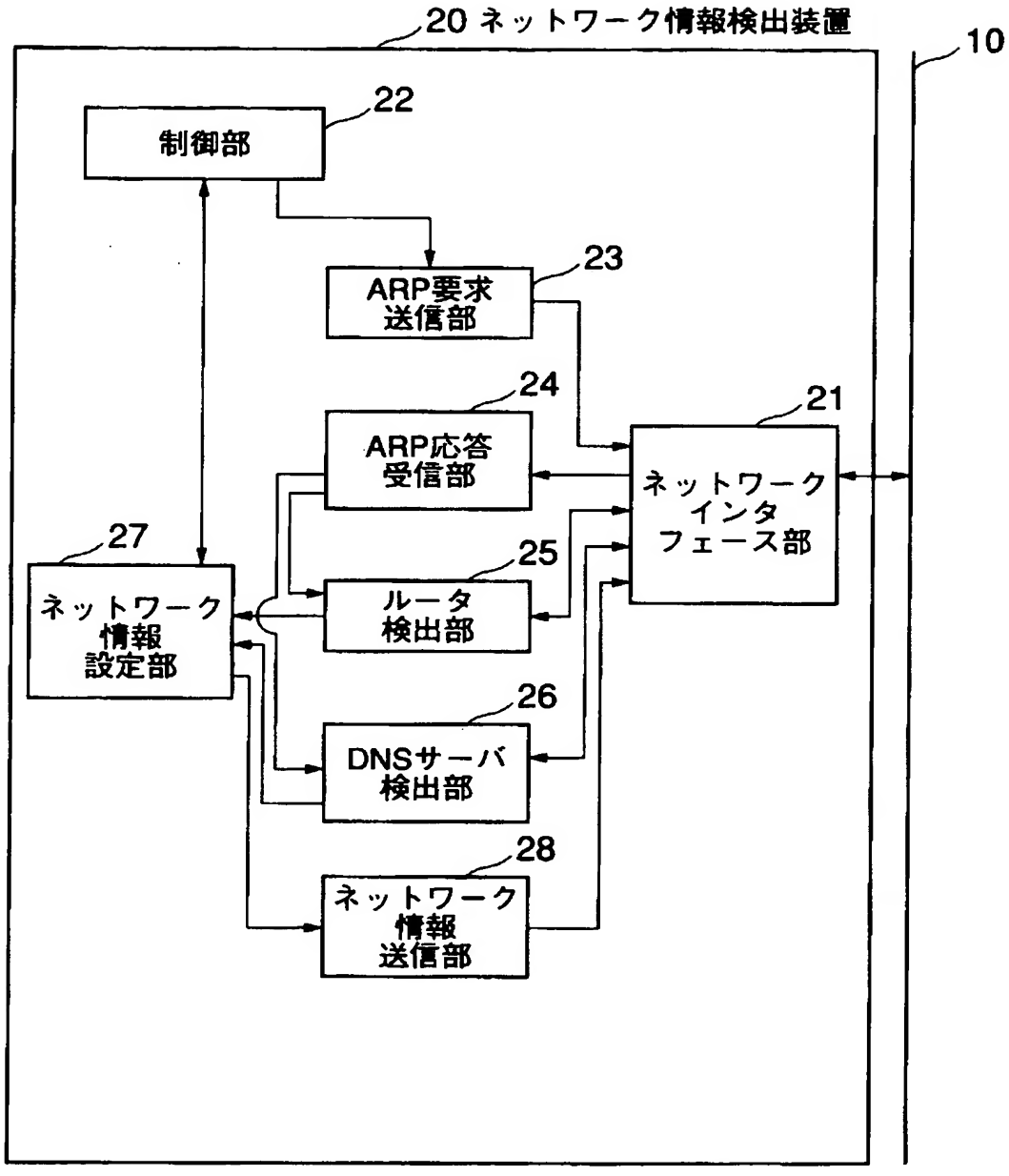
２７　ネットワーク情報設定部

【書類名】　図面

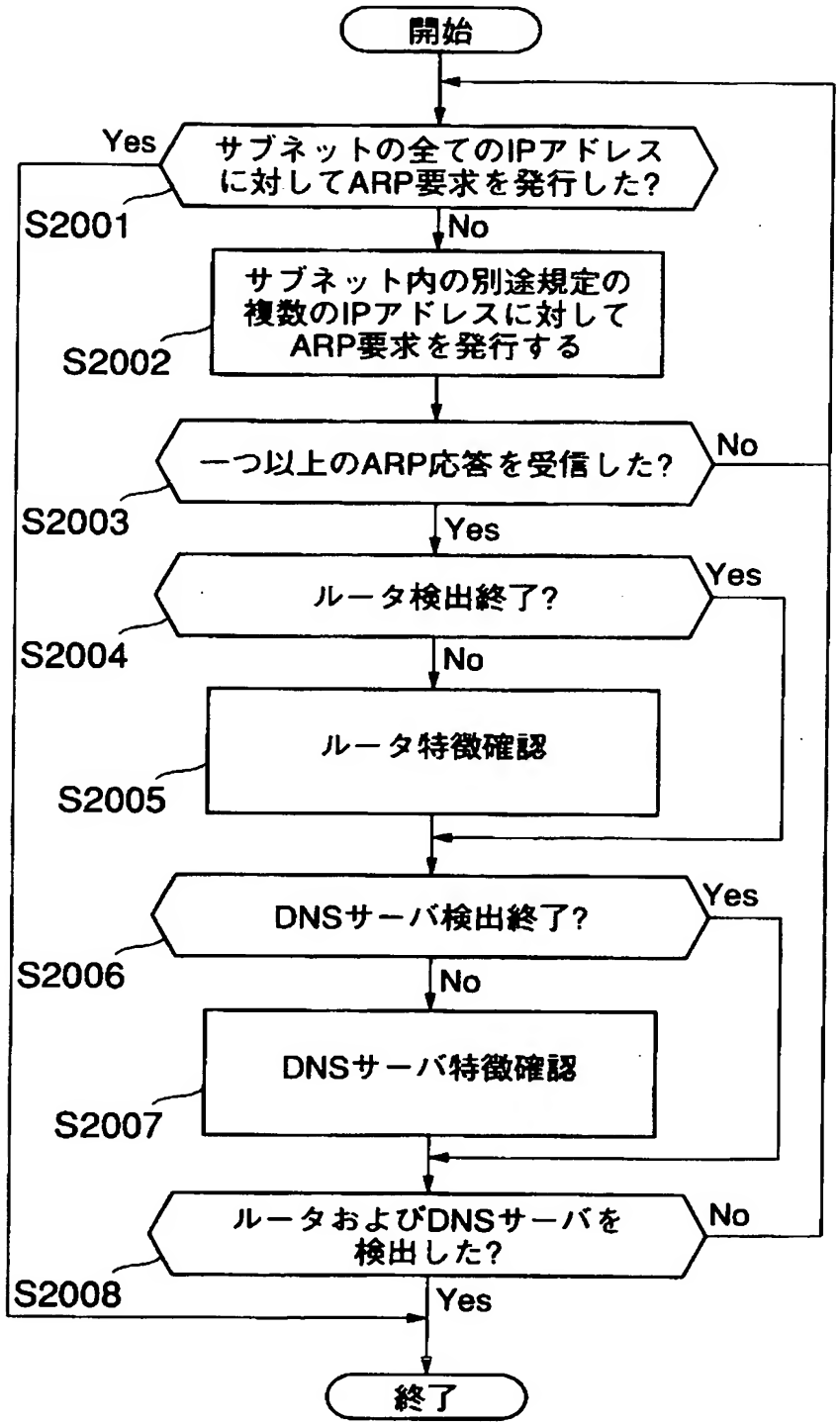
【図１】



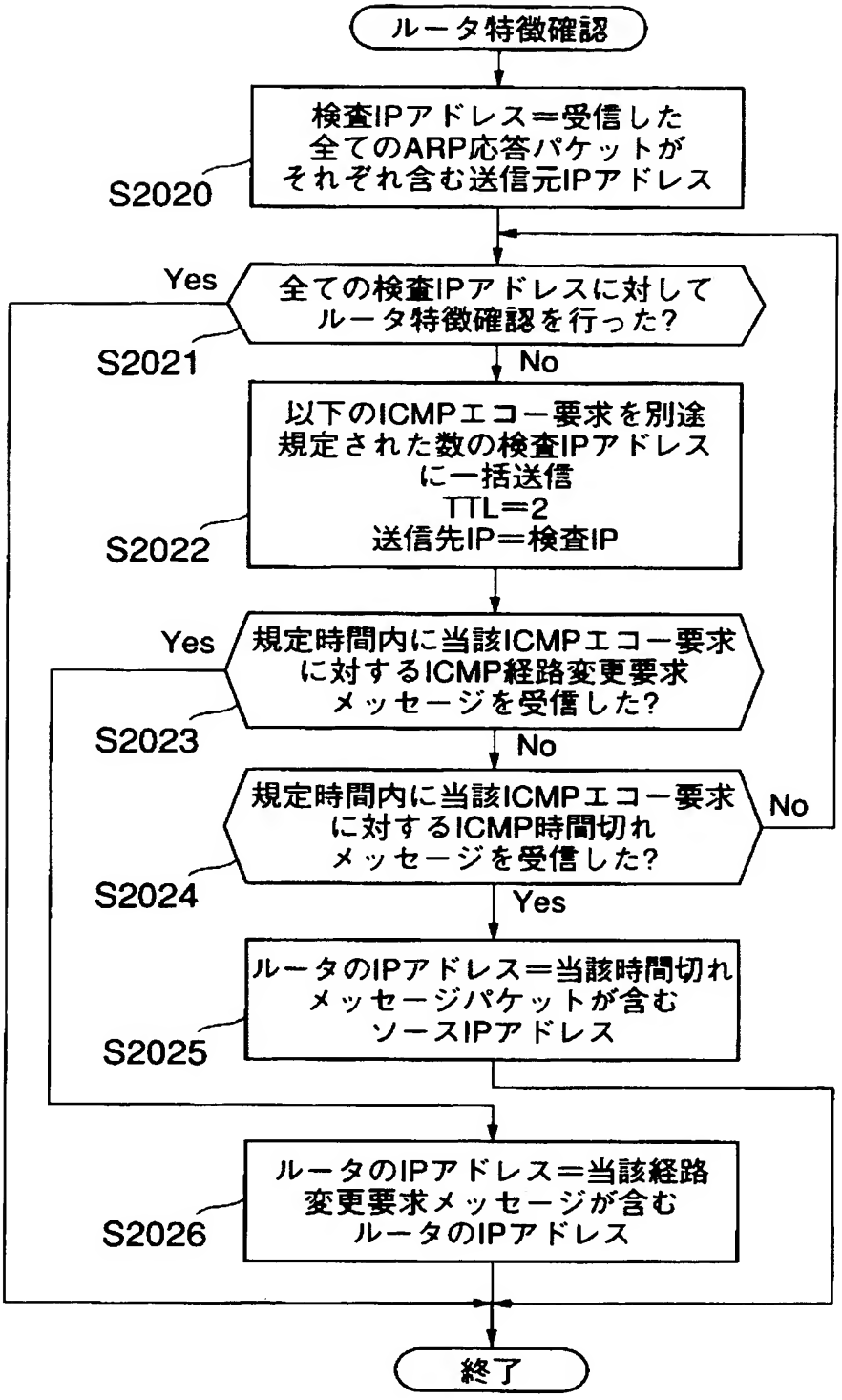
【図２】


20 ネットワーク情報検出装置
10
22
制御部
23
ARP要求
送信部
24
ARP応答
受信部
21
ネットワーク
インタ
フェース部
27
ネットワーク
情報
設定部
25
ルータ
検出部
26
DNSサーバ
検出部
28
ネットワーク
情報
送信部

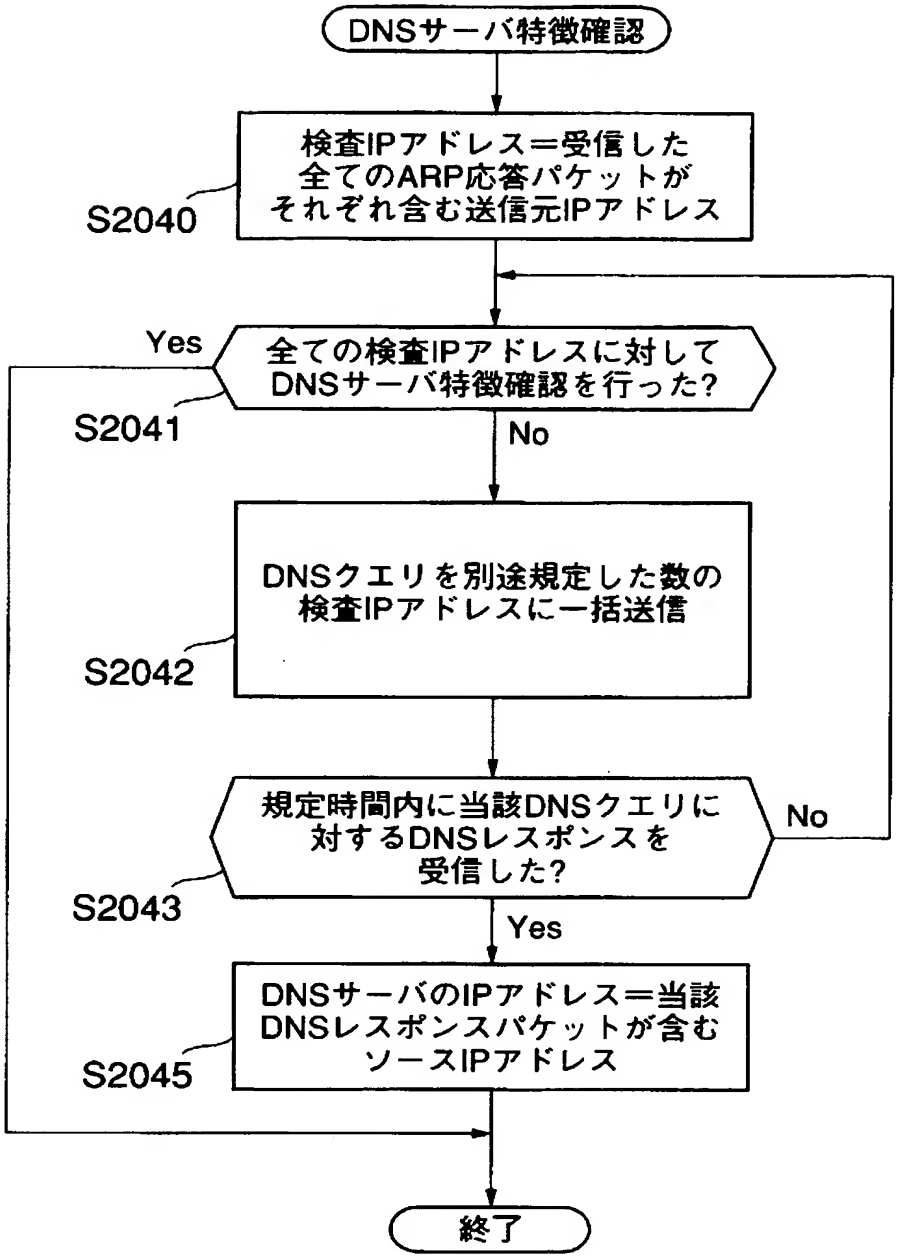
【図３】


開始
サブネットの全てのIPアドレス
に対してARP要求を発行した?
Yes
No
S2001
サブネット内の別途規定の
複数のIPアドレスに対して
ARP要求を発行する
S2002
一つ以上のARP応答を受信した?
No
Yes
S2003
ルータ検出終了?
Yes
No
S2004
ルータ特徴確認
S2005
DNSサーバ検出終了?
Yes
No
S2006
DNSサーバ特徴確認
S2007
ルータおよびDNSサーバを
検出した?
No
Yes
S2008
終了

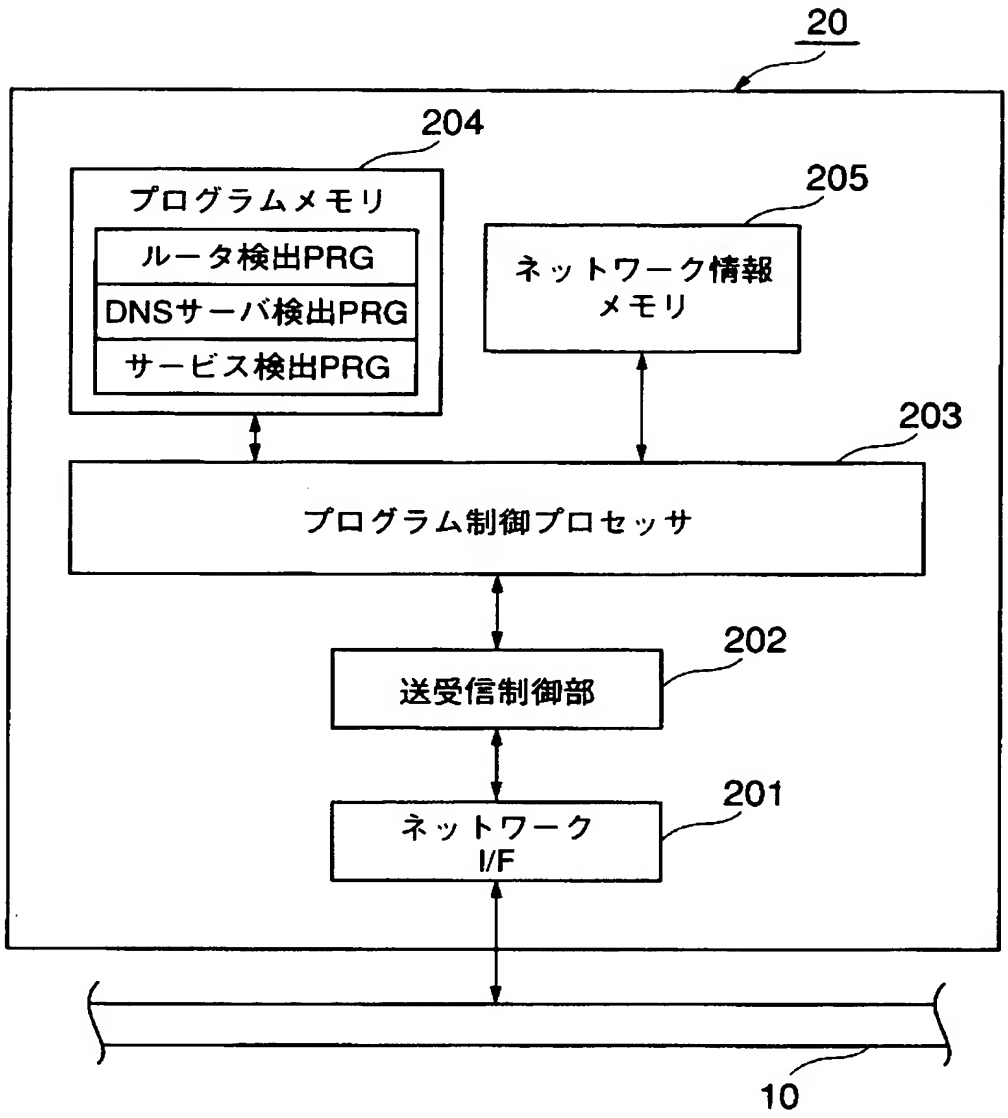
【図４】


ルータ特徴確認
検査IPアドレス＝受信した
全てのARP応答パケットが
それぞれ含む送信元IPアドレス
S2020
Yes
全ての検査IPアドレスに対して
ルータ特徴確認を行った?
S2021
No
以下のICMPエコー要求を別途
規定された数の検査IPアドレス
に一括送信
TTL＝2
送信先IP＝検査IP
S2022
Yes
規定時間内に当該ICMPエコー要求
に対するICMP経路変更要求
メッセージを受信した?
S2023
No
規定時間内に当該ICMPエコー要求
に対するICMP時間切れ
メッセージを受信した?
No
S2024
Yes
ルータのIPアドレス＝当該時間切れ
メッセージパケットが含む
ソースIPアドレス
S2025
ルータのIPアドレス＝当該経路
変更要求メッセージが含む
ルータのIPアドレス
S2026
終了

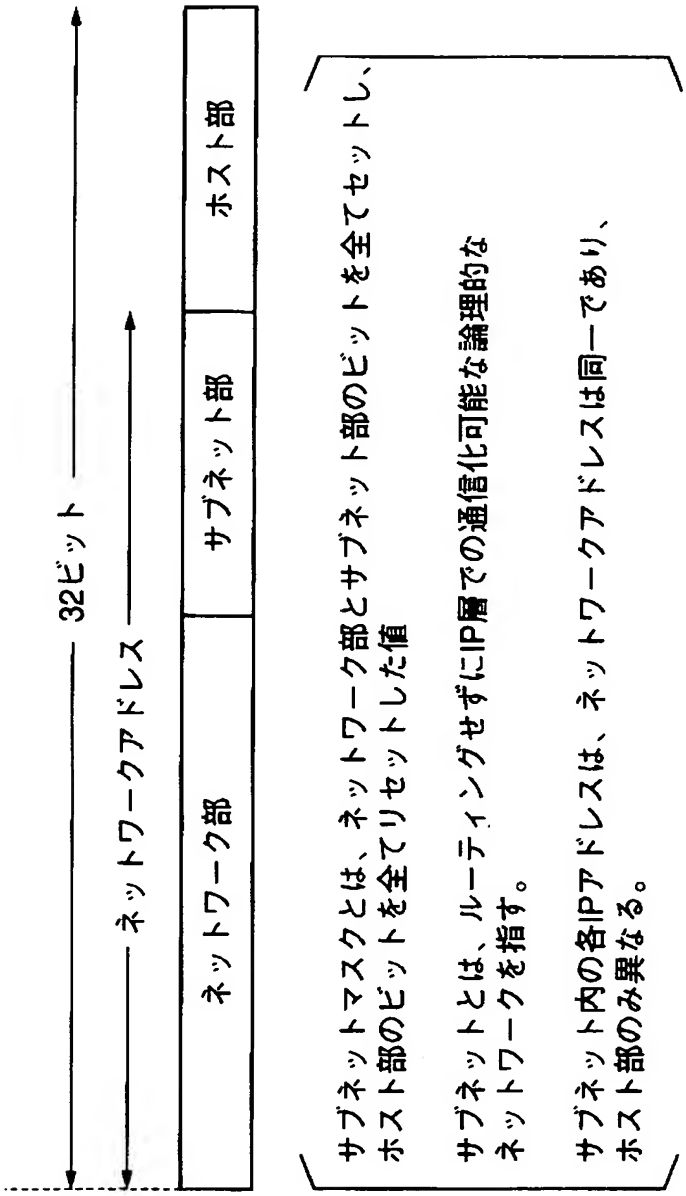
【図５】


DNSサーバ特徴確認
検査IPアドレス＝受信した全てのARP応答パケットがそれぞれ含む送信元IPアドレス
S2040
全ての検査IPアドレスに対してDNSサーバ特徴確認を行った?
Yes
S2041
No
DNSクエリを別途規定した数の検査IPアドレスに一括送信
S2042
規定時間内に当該DNSクエリに対するDNSレスポンスを受信した?
No
S2043
Yes
DNSサーバのIPアドレス＝当該DNSレスポンスパケットが含むソースIPアドレス
S2045
終了

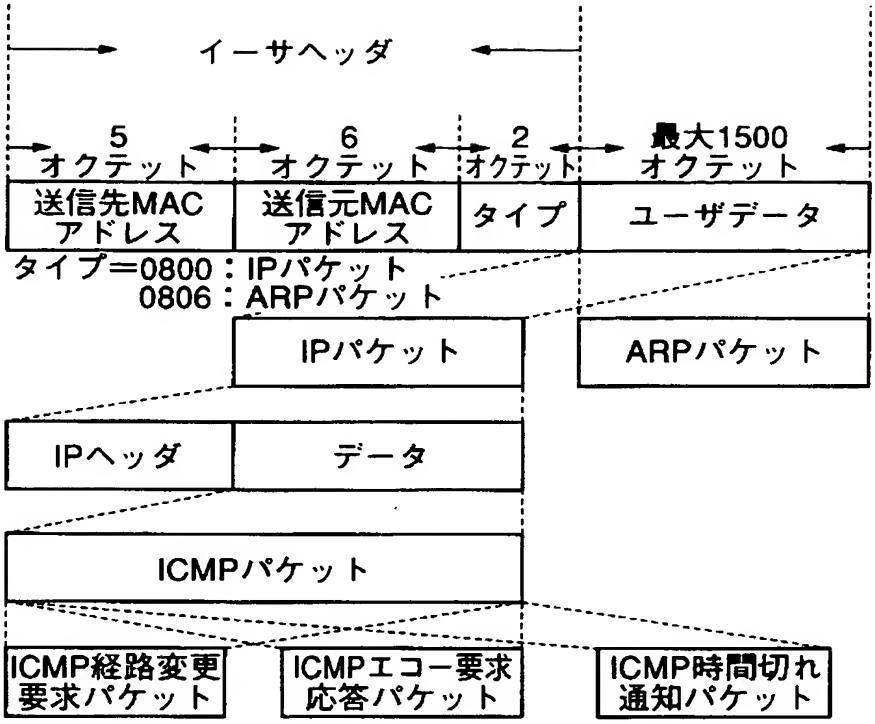
【図６】


20
204
プログラムメモリ
ルータ検出PRG
DNSサーバ検出PRG
サービス検出PRG
205
ネットワーク情報
メモリ
203
プログラム制御プロセッサ
202
送受信制御部
201
ネットワーク
I/F
10

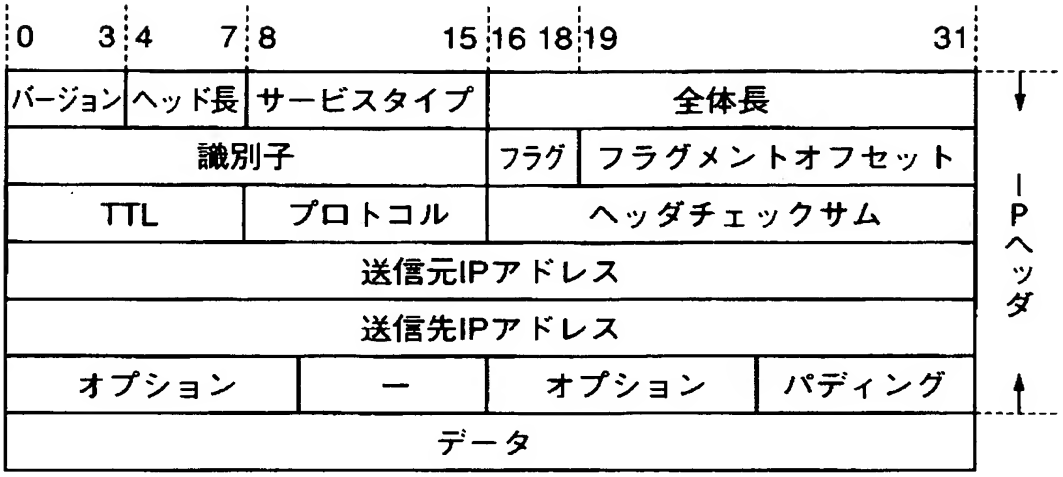
【図７】


32ビット
ネットワークアドレス
ネットワーク部
サブネット部
ホスト部
サブネットマスクとは、ネットワーク部とサブネット部のビットを全てセットし、
ホスト部のビットを全てリセットした値
サブネットとは、ルーティングせずにIP層での通信化可能な論理的な
ネットワークを指す。
サブネット内の各IPアドレスは、ネットワークアドレスは同一であり、
ホスト部のみ異なる。

【図８】


イーサヘッダ
5 オクテット
6 オクテット
2 オクテット
最大1500 オクテット
送信先MAC アドレス
送信元MAC アドレス
タイプ
ユーザデータ
タイプ＝0800：IPパケット
0806：ARPパケット
IPパケット
ARPパケット
IPヘッダ
データ
ICMPパケット
ICMP経路変更 要求パケット
ICMPエコー要求 応答パケット
ICMP時間切れ 通知パケット

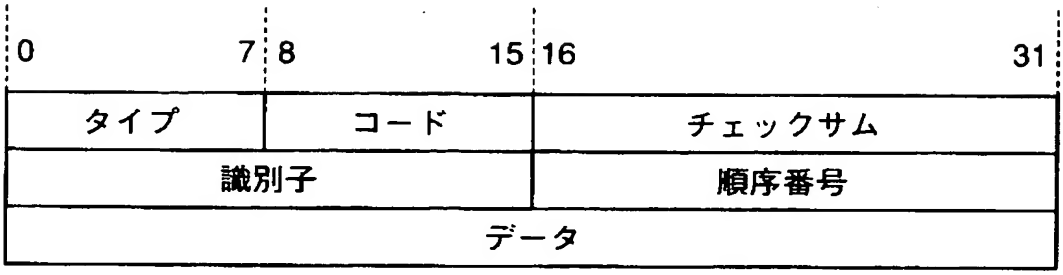
【図９】



プロトコル＝1：ICMP

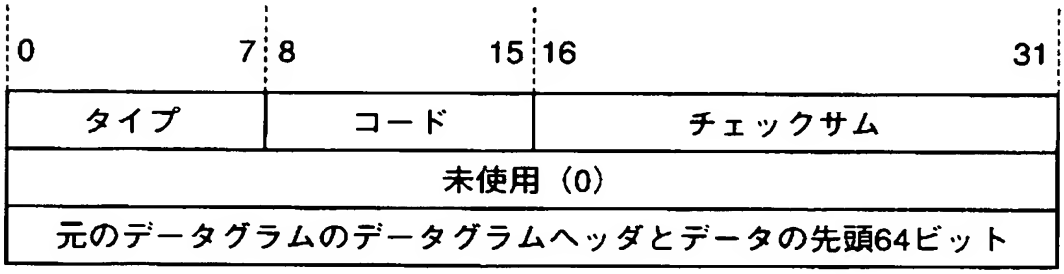
【図１０】

(A)



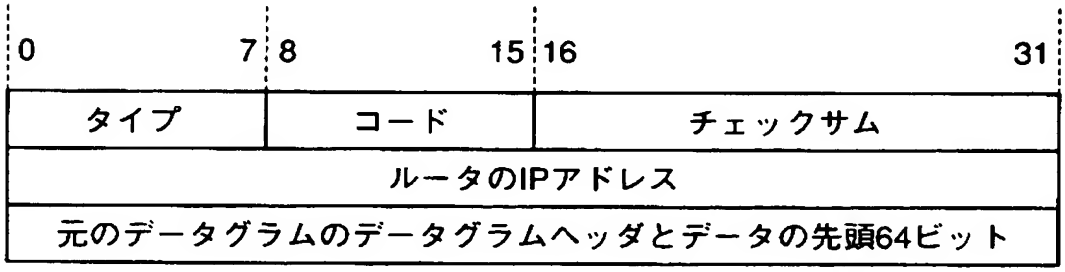
タイプ＝0：エコー応答（Echo Reply）
8：エコー要求（Echo Request）

(B)



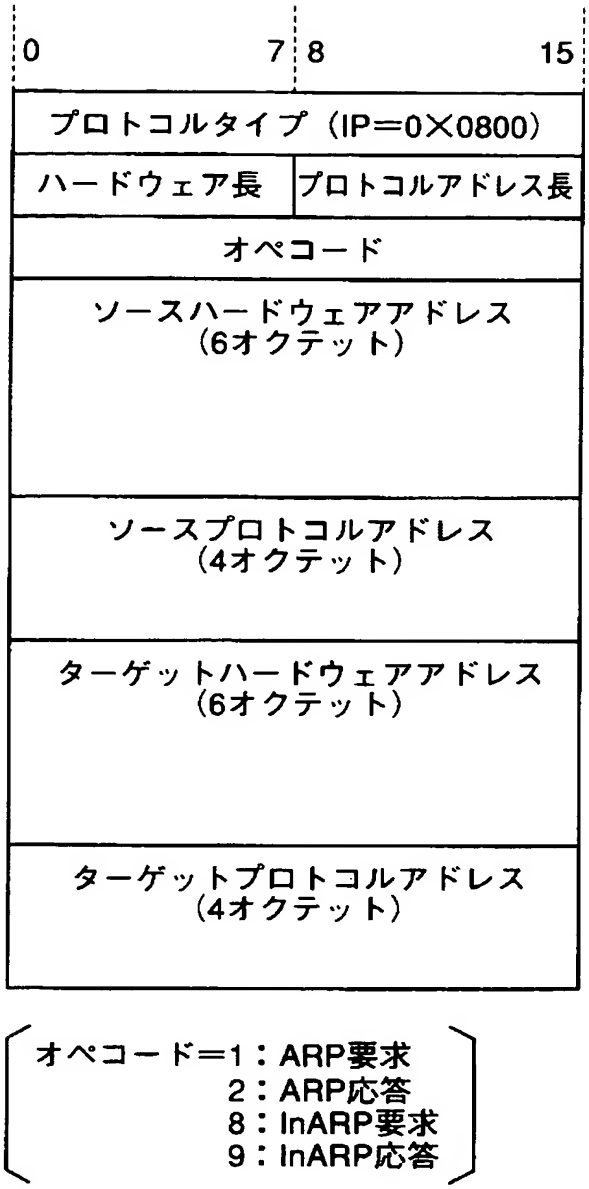
タイプ＝11：時間切れ（Time Exceeded for a Datagram）

(C)

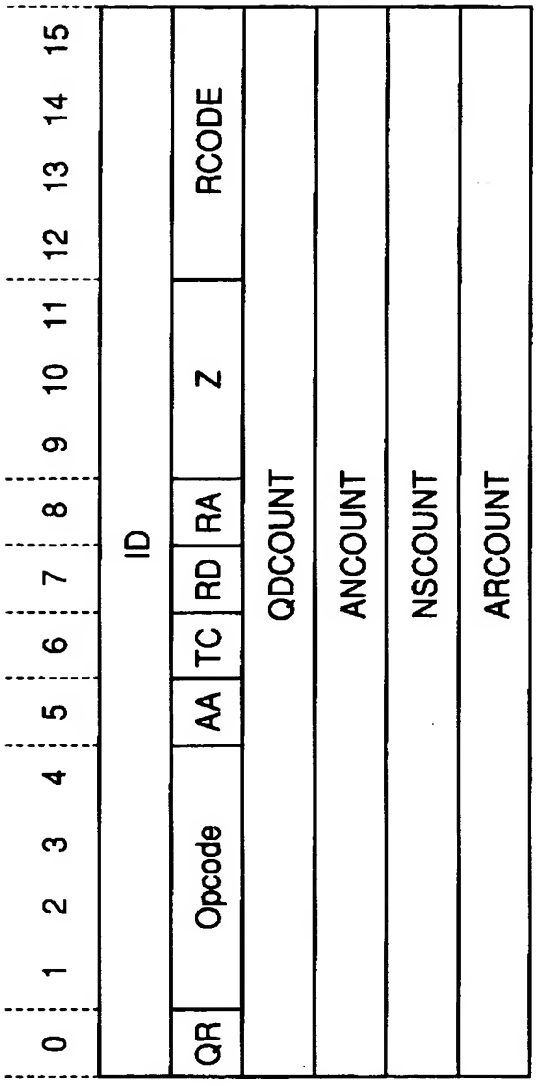


タイプ＝5：経路変更要求（Redirect）

【図１１】


0
7
8
15
プロトコルタイプ（IP＝0X0800）
ハードウェア長
プロトコルアドレス長
オペコード
ソースハードウェアアドレス
（6オクテット）
ソースプロトコルアドレス
（4オクテット）
ターゲットハードウェアアドレス
（6オクテット）
ターゲットプロトコルアドレス
（4オクテット）
オペコード＝1：ARP要求
2：ARP応答
8：InARP要求
9：InARP応答

【図１２】



ID　：　問い合わせを生成するプログラムによって割当てられた16ビット識別子。

QR　：　質問／回答　このメッセージが質問(0)か回答(1)かを示す1ビットフィールド。

OPCODE：このメッセージの質問の種類を示す4ビットフィールド。

0	a standard query (QUERY)
1	an inverse query (IQUERY)
2	a server status request (STATUS)
3・15	reserved for future use

【書類名】　要約書

【要約】

【課題】　ネットワーク情報を提供するサーバ機能を必要とせずに、ネットワーク情報を自動かつ高速で取得することができるネットワーク情報検出装置および方法を提供する。

【解決手段】　ネットワーク上の可能なＩＰアドレスから予め定められた個数ごとに選択されたＩＰアドレスから検査対象ＩＰアドレスを検出し、検出された検査対象ＩＰアドレスに対してＤＮＳクエリメッセージおよびＩＣＭＰエコー要求メッセージを一括送信する。それらのレスポンスメッセージからＤＮＳサーバおよびルータのＩＰアドレスを検出する。

【選択図】　図３

特願２００３－０７４８４６

出　願　人　履　歴　情　報

識別番号　［０００００４２３７］

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社